Chapitre II
Algorithmes de Chiffrement à Clés Publiques

Protocole Diffie-Hellman

Chiffrement de RSA

Chiffrement de Rabin

Chiffrement de Merkle-Hellman

Chiffrement de ElGamal

PROTOCOLE DE DIFFIE-HELLMAN

- Inventé par Whitfield Diffie et Martin Hellman en 1976

Whitfield Diffie

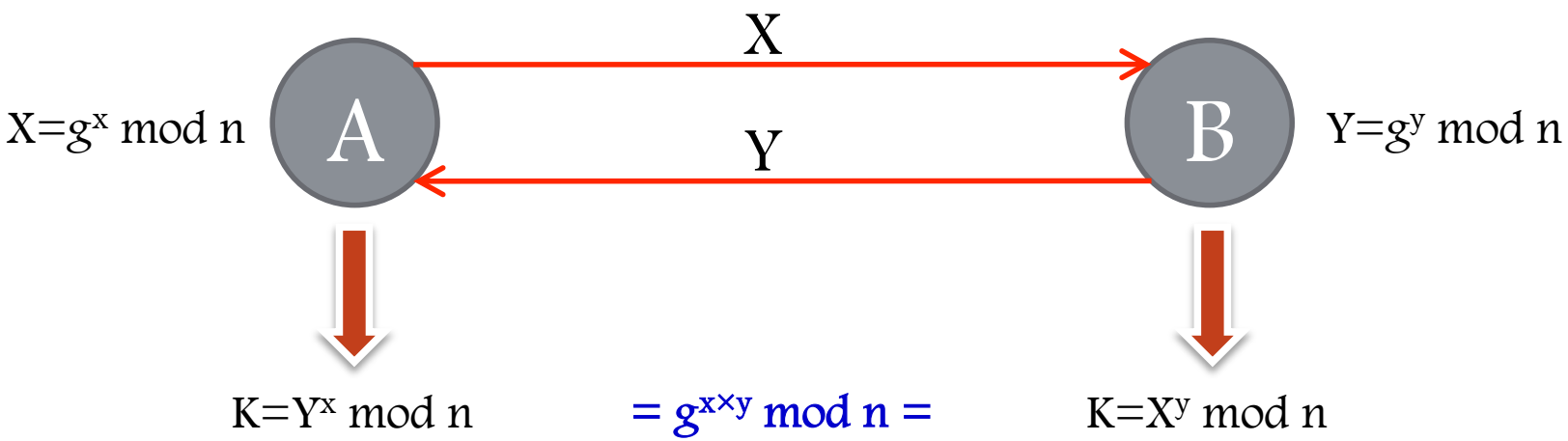
Martin Hellman

- La naissance de la cryptographie à clés asymétriques
- Partage d'une clé secrète par l'intermédiaire d'un échange de données publiques pouvant être interceptées
- Problème du Logarithme Discret ⇒ $A=B^X \bmod C$

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

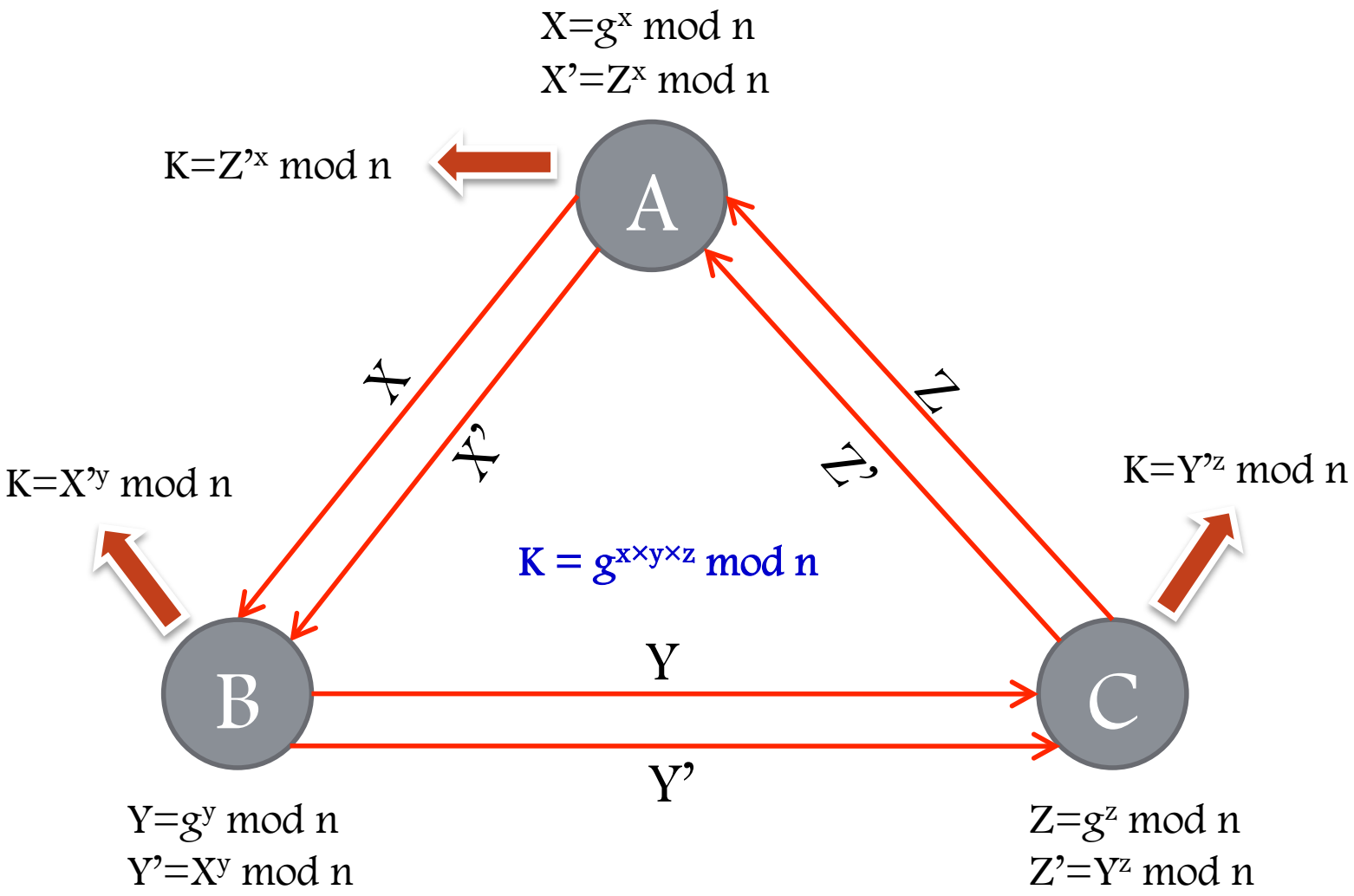
PROTOCOLE DE DIFFIE-HELLMAN

- A et B partagent deux paramètres (g, n) ⇒ publique
- Clé privée de A ⇒ x
- Clé privée de B ⇒ y
- L'intrus intercepte $X=g^x \bmod n$ **?!**



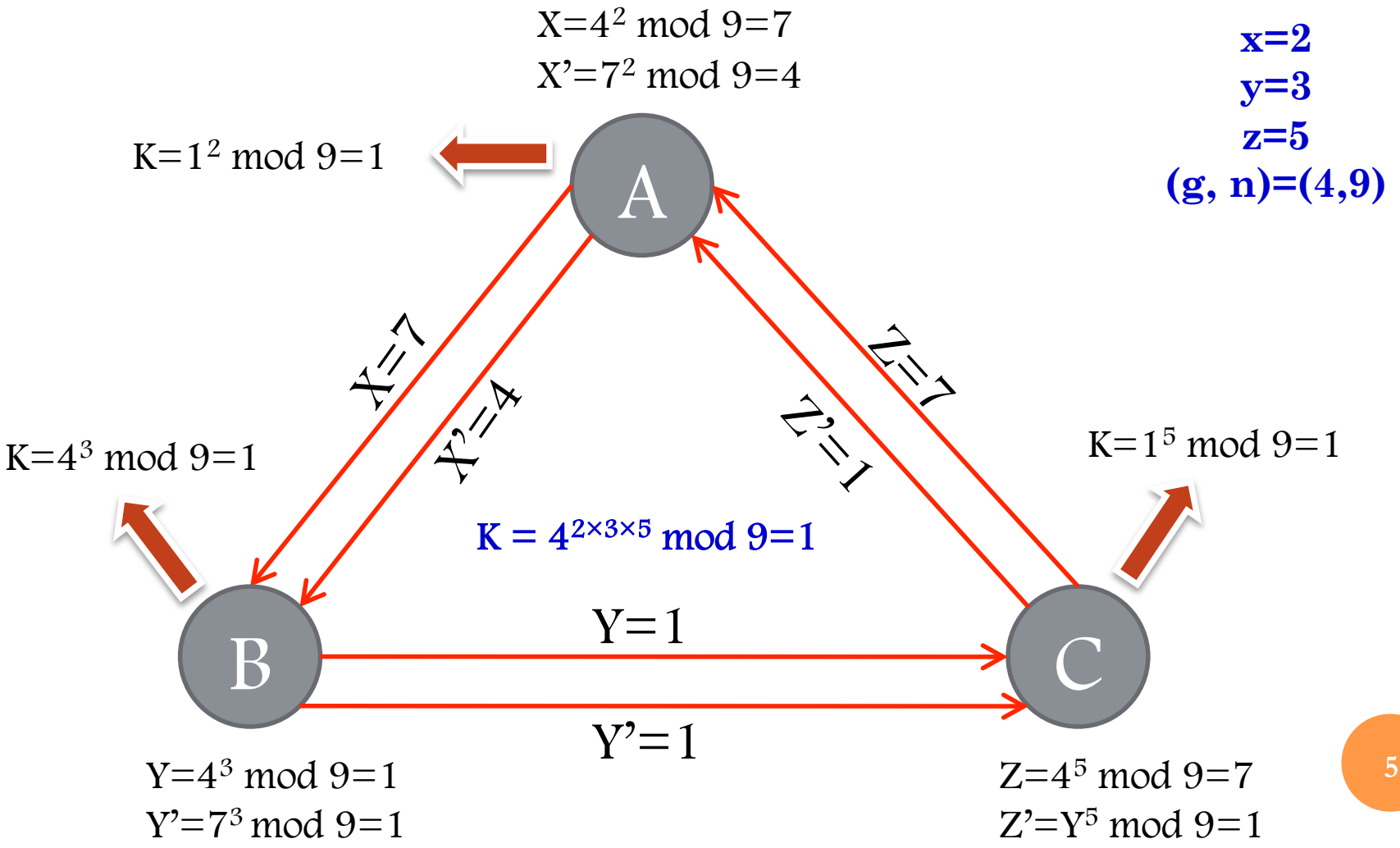
Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

PROTOCOLE DE DIFFIE-HELLMAN



Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

PROTOCOLE DE DIFFIE-HELLMAN

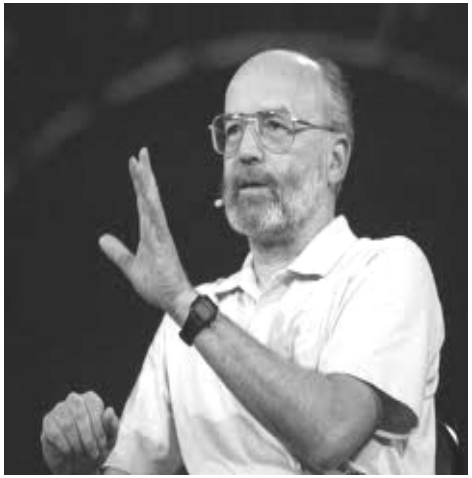


Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

CHIFFREMENT DE RSA

- Inventé par Ron Rivest, Adi Shamir et Leonard Adleman en 1977

Ronald Rivest



Adi Shamir

Leonard Adleman

- Le premier système de chiffrement à clés asymétriques
- Problème de factorisation

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

CHIFFREMENT DE RSA

- Choisir deux grands nombre premiers p et q
- Calculer $n=p\times q$
- Calculer $\phi(n)=(p-1)\times(q-1)$
- Choisir $e < \phi(n)$ tel que $pgcd(e, \phi(n))=1$
- Calculer d tel que $e\times d \bmod \phi(n)=1$
- Clé publique $\Rightarrow$ (e, n)
- Clé privée $\Rightarrow$ (d, n)
- Chiffrement $\Rightarrow C=M^e \bmod n$
- Déchiffrement $\Rightarrow M=C^d \bmod n$

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

CHIFFREMENT DE RABIN

- Inventé par Michael Rabin en 1979

Michael Rabin

- Amélioration du processus de chiffrement
- Problème de factorisation

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

CHIFFREMENT DE RABIN

- Choisir deux nombres premiers p et q :
  - $p \bmod 4 = 3$
  - $q \bmod 4 = 3$
- Clé publique $\Rightarrow n=p\times q$
- Clé privée $\Rightarrow (p, q)$
- Chiffrement $\Rightarrow C=M^2 \bmod n$
- Déchiffrement $\Rightarrow M=C^{1/2} \bmod n$
  - $m_p=C^{(p+1)/4} \bmod p$
  - $m_q=C^{(q+1)/4} \bmod q$
  - $p\times y_p + q\times y_q = 1$
  - $R=(p\times m_q\times y_p + q\times m_p\times y_q) \bmod n$
  - $S=(p\times m_q\times y_p - q\times m_p\times y_q) \bmod n$
  - Solutions possibles : $\{R, S, n-R, n-S\}$

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

CHIFFREMENT DE MERKLE-HELLMAN

- Inventé par Ralph Merkle et Martin Hellman en 1978

Ralph Merkle

Martin Hellman

- Nouvelle direction de chiffrement à clés asymétriques
- Problème du Sac-à-dos (*Knapsack problem*)

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

Problème de sac-à-dos avec une suite normale

1×	A	48 kg
0×	B	01 kg
0×	C	12 kg
1×	D	10 kg
1×	E	11 kg
1×	F	08 kg
0×	G	15 kg
1×	H	02 kg

SAC

Objet	Taille
A	48 kg
D	10 kg
E	11 kg
F	08 kg
H	02 kg
Poids total	79 kg

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

Problème de sac-à-dos avec une suite super-croissante

0×	A	96 kg
1×	B	39 kg
0×	C	20 kg
1×	D	11 kg
1×	E	05 kg
0×	F	02 kg
1×	G	01 kg

SAC

Objet	Taille	
B	39 kg	Reste 17 kg
D	11 kg	Reste 06 kg
E	05 kg	Reste 01 kg
G	01 kg	Reste 00 kg
Poids total	56 kg	

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

PROBLÈME DE SAC-À-DOS

- Etant donnée une suite A = $\{P_1, P_2, ..., P_k\}$ et un poids T. Est-il possible de trouver une suite de bits $b_1...b_k$ tel que

$$T = b_1 \times P_1 + b_2 \times P_2 + ... + b_k \times P_k$$

- Suite normale ⇒ le problème est NP-Difficile
- Suite super-croissante ⇒ il existe un algorithme polynomial permettant de calculer les b_i

Pour i=k **à** 1 **Faire**
  Si $T \geq P_i$ **Alors** $T := T - P_i$;
    $b_i := 1$;
  Sinon $b_i := 0$;
Fin pour
Si T = 0 **Alors** $\{b_1, b_2, \ldots, b_k\}$ est la solution ;
Sinon Il n'existe pas de solutions ;

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

RÉSOLUTION D'UNE SUITE SUPER-CROISSANTE

- A = {2, 3, 6, 13, 27, 52} pour T = 70

- $70 \geq 52 \Rightarrow T = 70-52 = 18$ — $b_6 = 1$
- $18 < 27 \Rightarrow$ — $b_5 = 0$
- $18 \geq 13 \Rightarrow T = 18-13 = 5$ — $b_4 = 1$
- $5 < 6 \Rightarrow$ — $b_3 = 0$
- $5 \geq 3 \Rightarrow T = 5-3 = 2$ — $b_2 = 1$
- $2 \geq 2 \Rightarrow T = 2-2 = 0$ — $b_1 = 1$

- $S = 110101_{(2)} = 53$

$1\times2 + 1\times3 + 0\times6 + 1\times13 + 0\times27 + 1\times52 = 70$

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

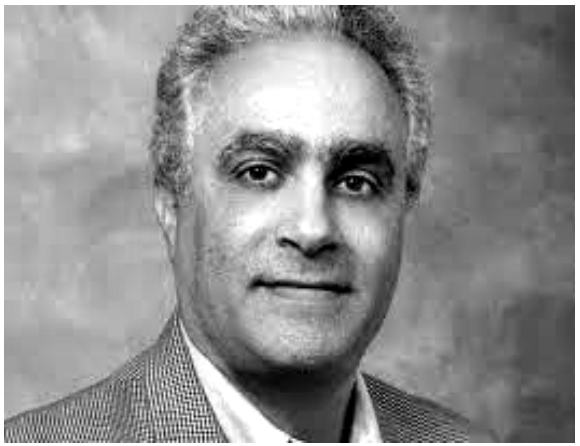
CHIFFREMENT DE MERKLE-HELLMAN

- Choisir une suite super-croissante $A = \{P_1, P_2, ..., P_k\}$
- Choisir deux nombres n et m :
  - $m > \sum P_i$
  - $pgcd(n, P_i) = 1$
- Calculer la suite $B = \{P'_1, P'_2, ..., P'_k\}$ tel que $P'_i = n \times P_i \bmod m$
- Clé publique $\Rightarrow$ B
- Clé privée $\Rightarrow$ (A, n, m)
- Chiffrement
  - $M = b_1 b_2 ... b_k$
  - $C = b_1 \times P'_1 + b_2 \times P'_2 + ... + b_k \times P'_k$
- Déchiffrement
  - Calculer n^{-1} tel que $n \times n^{-1} \bmod m = 1$
  - Calculer $T = n^{-1} \times C \bmod m$
  - Calculer les b_i avec l'algorithme de résolution de suite super-croissante

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

CHIFFREMENT D'ELGAMAL

- Inventé par Taher Elgamal en 1985



Taher Elgamal

- Concept hérité du protocole de Diffie-Hellman
- Permet le chiffrement et déchiffrement des messages
- Problème du Logarithme Discret

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

CHIFFREMENT D'ELGAMAL

- Choisir un grand nombre premier p et deux nombres a et g :
  - $a < p$
  - $g < p$
- Calculer $A=g^a \bmod p$
- Clé publique ⇒ (A, g, p)
- Clé privée ⇒ a
- Chiffrement
  - Choisir un nombre aléatoire b ($b < a$ et $pgcd(b, p-1)=1$)
  - Calculer $B=g^b \bmod p$
  - Calculer $C=M \times A^b \bmod p$
  - Le chiffré du message ⇒ (B, C)
- Déchiffrement ⇒ $M=C \times B^{p-a-1} \bmod p$

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

SIGNATURE NUMÉRIQUE AVEC RSA

- Paire de clés de l'expéditeur ⇒ {(e, n), (d, n)}
- Expéditeur ⇒ Génération de la signature de M
  - Calculer h=H(M)
  - Calculer $S=h^d \bmod n$
  - La signature numérique ⇒ (M, S)
- Destinataire ⇒ Vérification de la signature
  - Calculer h1=H(M)
  - Calculer $h2=S^e \bmod n$
  - Si h1=h2 ⇒ la signature est valide

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

SIGNATURE NUMÉRIQUE AVEC RABIN

- Paire de clés de l'expéditeur ⇒ {n, (p, q)}
- Expéditeur ⇒ Génération de la signature de M
  - Calculer h=H(M)
  - Calculer $\alpha = h^{1/2} \bmod n$
  - Choisir S parmi les quatre solutions possibles
  - La signature numérique ⇒ (M, S)
- Destinataire ⇒ Vérification de la signature
  - Calculer h1=H(M)
  - Calculer $h2 = S^2 \bmod n$
  - Si h1=h2 ⇒ la signature est valide

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

SIGNATURE NUMÉRIQUE AVEC MERKLE-HELLMAN

- Paire de clés de l'expéditeur ⇒ {B, (A, n, m)}
- Expéditeur ⇒ Génération de la signature de M
  - Calculer h=H(M)
  - Calculer n^{-1} et $T=n^{-1}\times h \bmod m$
  - Calculer les b_i
  - La signature numérique ⇒ (M, S) tel que $S=b_1b_2 \ldots b_k$
- Destinataire ⇒ Vérification de la signature
  - Calculer h1=H(M)
  - Calculer $h2 = b_1\times P'_1 + \ldots + b_k\times P'_k$
  - Si h1=h2 ⇒ la signature est valide

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia

SIGNATURE NUMÉRIQUE AVEC ELGAMAL

- Paire de clés de l'expéditeur ⇒ {(A, g, p), a}
- Expéditeur ⇒ Génération de la signature de M
  - Calculer h=H(M)
  - Choisir un nombre aléatoire b (b<a et pgcd(b, p−1)=1)
  - Calculer $B=g^b \bmod p$
  - Calculer C tel que $h=(a\times B+b\times C) \bmod (p-1)$
  - La signature numérique ⇒ (M, S) tel que S=(B, C)
- Destinataire ⇒ Vérification de la signature
  - Calculer h=H(M)
  - Si $A^B\times B^C \bmod p=g^h \bmod p$ ⇒ la signature est valide

Dr. OMAR Mawloud © 2015/2016 – Université de Béjaia